IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

VIRNETX INC. and LEIDOS, INC.,	§	
	§	
Plaintiffs,	§	
	§	
vs.	§	**CAUSE NO. 6:13-CV-351**
	§	
MICROSOFT CORPORATION,	§	
	§	
Defendant.	§	

MEMORANDUM OPINION AND ORDER

This Memorandum Opinion construes the disputed claim terms in U.S. Patent Nos. 6,502,135 ("the '135 Patent"), 7,188,180 ("the '180 Patent"), 7,418,504 ("the '504 Patent"), 7,490,151 ("the '151 Patent"), 7,921,211 ("the '211 Patent"), and 7,987,274 ("the '274 Patent") (collectively, "the patents-in-suit"). On September 4, 2014, the parties presented arguments on the disputed claim terms at a *Markman* hearing. For the reasons stated herein, the Court adopts the constructions set forth below.

BACKGROUND

Plaintiffs VirnetX Inc. and Leidos, Inc. (formerly Science Applications International Corporation) (collectively, "VirnetX") assert six patents against Defendant Microsoft Corporation ("Microsoft"). The '135 Patent discloses a method of transparently creating a virtual private network ("VPN") between a client computer and a target computer. The '504 and '211 Patents disclose a secure domain name service. The '151 Patent discloses a domain name service capable of handling both standard and non-standard domain name service queries. The '180 and '274 Patents disclose a method of establishing a secure communication link.

The patents-in-suit are all related; Application No. 09/504,783 ("the '783 Application") is an ancestor application for every patent-in-suit. The '135 Patent issued on December 31, 2002 from the '783 Application. The '151 Patent issued from a divisional of the '783 Application. The '180 Patent issued from a divisional of a continuation-in-part of the '783 Application. The '504 Patent issued from a continuation of a continuation-in-part of the '783 Application. The '211 Patent issued from a continuation of the application that resulted in the '504 patent. The '274 Patent issued from a continuation of a continuation of the application that resulted in the '180 Patent.

In other cases, the Court has already construed some of the terms at issue here. *See VirnetX Inc. v. Apple Inc.*, No. 6:12-cv-855, Docket No. 180 (E.D. Tex. Aug. 8, 2014) ("*Apple*"); *VirnetX Inc. v. Mitel Networks Corporation, et al.*, No. 6:11-cv-18, Docket No. 307 (E.D. Tex. Aug. 1, 2012) ("*Mitel*"); *VirnetX Inc. v. Cisco Systems, Inc., et al.*, No. 6:10-cv-417, Docket No. 266 (E.D. Tex. Apr. 25, 2012) ("*Cisco*"); *VirnetX Inc. v. Microsoft Corp.*, No. 6:07-cv-80, Docket No. 246 (E.D. Tex. July 30, 2009) ("*Microsoft I*"). The *Apple* and *Cisco* cases involved the '135, '504, '151, and '211 Patents; the *Mitel* case involved the '135, '504, and '211 Patents; and the *Microsoft I* case involved the '135 Patent.

APPLICABLE LAW

"It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Innova/Pure Water Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). In claim construction, courts examine the patent's intrinsic evidence to define the patented invention's scope. *See id.*; *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 861 (Fed. Cir. 2004); *Bell Atl. Network Servs., Inc. v. Covad*

Commc'ns Group, Inc., 262 F.3d 1258, 1267 (Fed. Cir. 2001). This intrinsic evidence includes the claims themselves, the specification, and the prosecution history. *See Phillips*, 415 F.3d at 1314; *C.R. Bard, Inc.*, 388 F.3d at 861. Courts give claim terms their ordinary and accustomed meaning as understood by one of ordinary skill in the art at the time of the invention in the context of the entire patent. *Phillips*, 415 F.3d at 1312–13; *Alloc, Inc. v. Int'l Trade Comm'n*, 342 F.3d 1361, 1368 (Fed. Cir. 2003).

The claims themselves provide substantial guidance in determining the meaning of particular claim terms. *Phillips*, 415 F.3d at 1314. First, a term's context in the asserted claim can be very instructive. *Id.* Other asserted or unasserted claims can also aid in determining the claim's meaning because claim terms are typically used consistently throughout the patent. *Id.* Differences among the claim terms can also assist in understanding a term's meaning. *Id.* For example, when a dependent claim adds a limitation to an independent claim, it is presumed that the independent claim does not include the limitation. *Id.* at 1314–15.

"[C]laims 'must be read in view of the specification, of which they are a part.'" *Id.* (quoting *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc)). "[T]he specification 'is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.'" *Id.* (quoting *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996)); *see also Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002). This is true because a patentee may define his own terms, give a claim term a different meaning than the term would otherwise possess, or disclaim or disavow the claim scope. *Phillips*, 415 F.3d at 1316. In these situations, the inventor's lexicography governs. *Id.* Also, the specification may resolve ambiguous claim terms "where the ordinary and accustomed meaning of the words used in the claims lack

sufficient clarity to permit the scope of the claim to be ascertained from the words alone." *Teleflex, Inc.*, 299 F.3d at 1325. But, "'[a]lthough the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims.'" *Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (quoting *Constant v. Advanced Micro-Devices, Inc.*, 848 F.2d 1560, 1571 (Fed. Cir. 1988)); *see also Phillips*, 415 F.3d at 1323. The prosecution history is another tool to supply the proper context for claim construction because a patent applicant may also define a term in prosecuting the patent. *Home Diagnostics, Inc., v. Lifescan, Inc.*, 381 F.3d 1352, 1356 (Fed. Cir. 2004) ("As in the case of the specification, a patent applicant may define a term in prosecuting a patent.").

Although extrinsic evidence can be useful, it is "'less significant than the intrinsic record in determining the legally operative meaning of claim language.'" *Phillips*, 415 F.3d at 1317 (quoting *C.R. Bard, Inc.*, 388 F.3d at 862). Technical dictionaries and treatises may help a court understand the underlying technology and the manner in which one skilled in the art might use claim terms, but technical dictionaries and treatises may provide definitions that are too broad or may not be indicative of how the term is used in the patent. *Id.* at 1318. Similarly, expert testimony may aid a court in understanding the underlying technology and determining the particular meaning of a term in the pertinent field, but an expert's conclusory, unsupported assertions as to a term's definition is entirely unhelpful to a court. *Id.* Generally, extrinsic evidence is "less reliable than the patent and its prosecution history in determining how to read claim terms." *Id.*

LEVEL OF ORDINARY SKILL IN THE ART

The parties agree that a person of ordinary skill in the art would have a master's degree in computer science or computer engineering as well as two years of experience in computer networking and computer network security.

AGREED CLAIM TERMS

In the Joint Claim Construction Chart (Docket No. 83-1, Ex. A) the parties agreed to the construction of the following terms:

Claim Term	Agreed Construction
secure target web site	a secure web site on the target computer
automatically initiating the VPN	initiating the VPN without involvement of a user
secure computer network address	a network address that requires authorization for access and is associated with a computer capable of virtual private network communications
automatically initiating an encrypted channel / automatically creating an encrypted channel / automatically creating a secure channel	[initiating/creating] the [encrypted channel/secure channel] without involvement of a user
secure server	a server that requires authorization for access and that can communicate in an encrypted channel
enable establishment of a secure communication link . . . transparently to a user at the first location	the user at the first location need not be involved in enabling establishment of the secure communication link
secure network address	a network address that requires authorization for access and is associated with a computer capable of virtual private network communications

DISPUTED CLAIM TERMS

virtual private network (VPN)

Asserted claims of the '135 Patent, the '180 Patent, and the '274 Patent contain the term "virtual private network" or "VPN." VirnetX proposes "a network of computers which privately

and directly communicate with each other by encrypting traffic on insecure communication paths between the computers." Microsoft proposes "a network of computers which privately and directly communicate with each other as though they were on the same network by encrypting traffic on insecure paths between computers where the communication is both secure and anonymous." The Court previously construed this term in *Apple*, *Mitel*, *Cisco*, and *Microsoft I*.[1] The parties now raise two disputes regarding the construction of VPN.

First, the parties dispute whether the VPN must be both secure and anonymous. Microsoft argues that a construction requiring anonymity is now well settled. Docket No. 101 at 3–4. Therefore, Microsoft urges the Court to adopt the anonymity requirement from its previous constructions in *Cisco* and *Mitel*. *Id.* VirnetX argues, as it did in the *Apple* case, that the "private" aspect of a VPN does not require anonymity. Docket No. 95 at 2. VirnetX incorporates by reference its arguments in *Apple*. *Id.*; *Apple*, Docket No. 136 at 10.

The Court's claim construction order in *Microsoft I* made clear that this term requires anonymity, even though the Court did not expressly include the anonymity requirement in its construction. *See Microsoft I*, Docket No. 246 at 9 ("[T]he Court construes 'virtual private network' as requiring both data security and anonymity."). For clarity, the Court explicitly added the anonymity requirement to its later constructions of this term in *Cisco* and *Mitel*. *See, e.g.*, *Cisco*, Docket No. 266 at 5. The Court hereby incorporates by reference its reasoning in *Microsoft I*. For the reasons stated in *Microsoft I* and adopted in *Cisco*, *Mitel*, and *Apple*, the Court finds that a VPN requires anonymity. *See Microsoft I*, Docket No. 246 at 8–9.

[1] In *Microsoft I*, the Court construed "virtual private network" as "a network of computers which privately communicate with each other by encrypting traffic on insecure communication paths between the computers." *Microsoft I*, Docket No. 246 at 4–10. In *Cisco*, *Mitel*, and *Apple*, the Court construed "virtual private network" as "a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between the computers where the communication is both secure and anonymous." *Apple*, Docket No. 180 at 8; *Mitel*, Docket No. 307 at 4–6; *Cisco*, Docket No. 266 at 5–8.

Second, the parties dispute whether a VPN requires communication between computers "as though they were on the same network." Microsoft argues that its proposed construction merely adopts what VirnetX has repeatedly acknowledged. Docket No. 101 at 4–5. Microsoft also argues that this requirement was advanced during reexamination to distinguish the Aventail reference. *Id.* at 4. VirnetX argues that Microsoft's proposal is redundant because "private" means that a computer outside of a private network can communicate as if it were physically within that private network. Docket No. 95 at 3.

At the hearing, Microsoft and VirnetX acknowledged that "directly," a term used in both parties' proposed constructions, may be synonymous with "as though they were on the same network." Tr. Sep. 4, 2014, Docket No. 124 at 11:24–12:8, 16:6–14. Microsoft asks the Court to include both terms for the sake of clarity. *Id.* at 15:23–16:6. VirnetX argues that instead of clarifying the issue, a construction including both "directly" and "as though they were on the same network" would suggest that the terms actually have different meanings. *Id.* at 18:23–19:6. According to VirnetX, Microsoft's proposal would invite ambiguity for a jury determining whether the computers are communicating "as though they were on the same network." *Id.* at 11:5–15. Based on the parties' concessions, the Court agrees that a construction that includes both "directly" and "as though they were on the same network" would not be clearer than the Court's previous constructions.

For the reasons stated in *Apple*, *Mitel*, *Cisco*, and *Microsoft I* and subject to the above clarifications, the Court construes "virtual private network" as "a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between the computers where the communication is both secure and anonymous."

Domain Name Service (DNS)

Asserted claims of the '135 Patent, the '180 Patent, the '504 Patent, and the '211 Patent contain the term "domain name service" or "DNS." VirnetX proposes "a lookup service that returns an IP address for a requested domain name." Microsoft proposes "a lookup service, which includes a modified and conventional DNS server function, that returns an IP address for a requested domain name to the requester." The Court previously construed this term in *Cisco* and *Microsoft I*.[2] The parties now raise two disputes regarding the proper construction of DNS.

First, the parties disagree about whether the IP address must be returned "to the requester." VirnetX argues that the Court should adopt its construction from *Microsoft I*. Docket No. 95 at 3–4. VirnetX objects to the addition of the phrase "to the requester" for the same reasons it raised in *Cisco*. *Id.* Microsoft's proposal adopts the Court's construction in *Cisco*. Docket No. 101 at 5–6.

In *Microsoft I*, the parties did not raise the issue of whether the IP address must be returned "to the requester." The Court subsequently added the "to the requester" limitation after the parties presented arguments in *Cisco*. *Cisco*, Docket No. 266 at 14–15. Because VirnetX raises no new argument that was not considered in *Cisco*, the Court includes "to the requester" in the construction.

Second, the parties dispute whether the ordinary meaning of DNS includes, or necessarily requires, that both a conventional DNS server function and a modified DNS server function be present. Microsoft urges inclusion of both features. *Id.* at 6. In support, Microsoft identifies VirnetX's characterizations of the claimed DNS server functions as going beyond a

[2] In *Microsoft I*, the Court construed "Domain Name Service" as "a lookup service that returns an IP address for a requested domain name." *Microsoft I*, Docket No. 246 at 12. Subsequently, in *Cisco*, the Court construed "Domain Name Service" as "a lookup service that returns an IP address for a requested domain name to the requester." *Cisco*, Docket No. 266 at 14–15.

"conventional" DNS. *Id.* at 6–7. Microsoft also points to Figure 26 of the patent specification as disclosing a modified DNS. *Id.* at 7. VirnetX argues that Microsoft's proposal reflects features of a modified DNS rather than the ordinary meaning of the term DNS. Docket No. 95 at 4.

Microsoft improperly conflates the structure of a preferred embodiment DNS server used to perform the method of the '135 Patent claims with an actual claim limitation. *See Comark Commc'ns, Inc.*, 156 F.3d at 1187 ("Although the specification may aid the court in interpreting the meaning of disputed claim language, particular embodiments and examples appearing in the specification will not generally be read into the claims."). Accordingly, the Court construes "domain name service" or "DNS" as "a lookup service that returns an IP address for a requested domain name to the requester."

secure domain name

Asserted claims of the '180 Patent and the '274 Patent contain the term "secure domain name." VirnetX proposes "a non-standard domain name that corresponds to a secure computer network address and cannot be resolved by a conventional DNS." Microsoft proposes "a non-standard top-level domain name that corresponds to a secure computer network address."

VirnetX argues that its construction tracks the agreed-upon construction in *Cisco* and VirnetX's use of the term during reexamination. Docket No. 95 at 5. VirnetX contends that Microsoft's construction improperly specifies a top-level domain name. *Id.* at 5–6. According to VirnetX, the term may designate a top-level domain name, but does not necessarily do so. *Id.* Microsoft responds that the scope of the specification is no broader than a secure domain name that is a non-standard top-level domain name. Docket No. 101 at 8–10. Microsoft also argues that claim 11, which depends from claim 1 and recites a subset of top-level domain names,

would have no antecedent basis if claim 1 did not refer to only top-level domain names. *Id.* at 10–11.

The U.S. Court of Appeals for the Federal Circuit considered a related term in *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1316 (Fed. Cir. 2014). There, the Federal Circuit examined the proper construction of "domain name" as used in claims of the '504 and '211 Patents. *Id.* at 1316. Referring to applications described in the specifications, the Court explained that "[t]he disclosure of such applications demonstrates that the inventors did not intend to limit 'domain name' to the particular formatting limitations of websites sought by Apple, i.e., a top-level domain, second-level domain, and host name." *Id.* The Federal Circuit also declined to read a hierarchical limitation into the independent claims on the basis of claim differentiation. *Id.* at 1317 (noting that the dependent claims include the "top-level domain name" limitation and that the independent claims do not).

The Federal Circuit did not confront precisely the same arguments and claims as the parties have argued in this case. However, the '180 Patent here shares a specification with the patents described in the Federal Circuit opinion. The Court therefore adopts the reasoning used by the Federal Circuit in construing "domain name" and rejects Microsoft's argument that the "top-level" requirement should be included. The Court construes "secure domain name" as "a non-standard domain name that corresponds to a secure computer network address."

secure domain name service

Asserted claims of the '180 Patent and the '274 Patent contain the term "secure domain name service." VirnetX proposes "a non-standard lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name." Microsoft proposes "a non-standard lookup service that

interfaces with existing applications and recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name." The Court previously construed this term in *Cisco*.[3]

VirnetX argues that the Court should adopt its construction from *Cisco*. Docket No. 95 at 6. VirnetX objects to Microsoft's contention that a secure domain name service must also "interface with existing applications." *Id.* at 7–8. VirnetX alleges that the proposed limitation is neither a disclaimer nor a definition, but instead merely a description from the summary of the invention. *Id.* at 7. Microsoft contends that the summary of the invention section of the specification narrows the scope of the claims because it describes the invention as a whole using the language "according to the invention." Docket No. 101 at 11–13.

The Court adopts its previous construction of the term from *Cisco.* The ability to interface with existing applications is merely a capability of the disclosed secure domain name service. Microsoft points to nothing in the specification that indicates that such a capability is a necessary aspect of accessing a secure computer network. Instead, Microsoft identifies a generalized reference to operational capabilities of the disclosed embodiments:

> The present invention provides key technologies for implementing a secure virtual Internet by using a new agile network protocol that is built on top of the existing Internet protocol (IP). . . . According to the invention, the secure domain name service interfaces with existing applications, in addition to providing a way to register and serve domain names and addresses.

Accordingly, the Court construes "secure domain name service" as "a non-standard lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name."

[3] In *Cisco*, the Court construed "secure domain name service" as "a non-standard lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name." *Cisco*, Docket No. 266 at 17–19.

DNS proxy server

Asserted claims of the '135 Patent contain the term "DNS proxy server." VirnetX proposes "a computer or program that responds to a domain name inquiry in place of a DNS." Microsoft proposes "a computer or program, separate from the client, that responds to a domain name inquiry in place of a DNS." The Court previously construed this term in *Microsoft I*, *Cisco*, and *Mitel*.[4]

VirnetX argues that the Court should adopt its previous constructions of this term. Docket No. 95 at 9. VirnetX objects to Microsoft's construction because it would require that the DNS proxy server and the DNS proxy module be "separate from the client." *Id.* In response, Microsoft amends its construction to state "separate from the client application" rather than "separate from the client." Docket No. 101 at 13–14. Microsoft argues that under the claim language of the '135 Patent, the DNS proxy server makes a determination on a DNS request "transmitted" by the client computer and "receives a request from the client computer." *Id.* at 14. Microsoft argues that the claimed proxy server cannot adhere to those plain language requirements unless the proxy server is at least separate from the client application. *Id.*

At the hearing in this case, the Court asked VirnetX whether the amendment to "separate from the client application" resolves VirnetX's objection. Tr. Sep. 4, 2014, Docket No. 124 at 38:24–39:4. VirnetX conceded that the proposal at least partially addressed its concerns but continued to object that the amendment is insufficient and the limitation is inappropriate. *Id.* at 39:17–19.

[4] In all three cases, the Court construed "DNS proxy server" as "a computer or program that responds to a domain name inquiry in place of a DNS." *Mitel*, Docket No. 347 at 8; *Cisco*, Docket No. 266 at 17; *Microsoft I*, Docket No. 246 at 24.

Although the client computer can perform the determining step,[5] there is an inherent separation between a client application that sends a DNS request and a program that receives the request. The claim language itself so specifies. Accordingly, the Court construes "DNS proxy server" as "a computer or program, separate from the client application, that responds to a domain name inquiry in place of a DNS."

domain name server (DNS) proxy module

Asserted claims of the '151 Patent contain the term "domain name server (DNS) proxy module." VirnetX proposes "a computer module or program module that responds to a domain name inquiry in place of a DNS." Microsoft proposes "a program, separate from the client, that responds to a domain name inquiry in place of a DNS."

The issue and arguments regarding this term are identical to those raised for the previous term ("DNS proxy server"). Therefore, for the same reasons set forth above, the Court construes "domain name server (DNS) proxy module" as "a computer module or program module, separate from the client application, that responds to a domain name inquiry in place of a DNS."

generating from the client computer a Domain Name Service (DNS) request

Asserted claims of the '135 Patent contain the term "generating from the client computer a Domain Name Service (DNS) request." VirnetX argues that no construction is necessary. Microsoft proposes "generating and transmitting from the client computer a DNS request." The Court previously construed this term in *Apple*, *Mitel*, *Cisco*, and *Microsoft I*.[6]

This term appears in the first step of the method recited in claim 1 of the '135 Patent. In that first step, a DNS request is generated from the client computer. The second step determines

[5] The Court previously found that "[t]he client computer can perform the 'determining' step." *Microsoft I*, Docket No. 246 at 20.

[6] In all four cases, the Court construed "generating from the client computer a Domain Name Service (DNS) request" as "generating and transmitting from the client computer a DNS request." *Apple*, Docket No. 180 at 8; *Mitel*, Docket No. 347 at 8; *Cisco*, Docket No. 266 at 17; *Microsoft I*, Docket No. 246 at 24.

whether the DNS request seeks access to a secure web site. In *Apple*, the parties agreed that the second step could be performed by either a separate device or the client computer. *Apple*, Docket No. 180 at 8. Given that understanding, the Court in *Apple* adopted the parties' agreed construction. *Id.* At the hearing in this case, the Court asked the parties whether they would be amenable to a similar agreement. Tr. Sep. 4, 2014, Docket No. 124 at 55:18–24. VirnetX expressed willingness to reach an agreement, but Microsoft objected. *Id.* at 55:25–56:4. Microsoft expressed concern that the rationale underlying Apple's agreement was unclear; thus, Microsoft could not make the same agreement. *Id.* at 56:2–4.

Although VirnetX and Microsoft were unable to agree on a construction in this case, the Court adopts its previous constructions. With the understanding that this construction does not preclude the client device from performing the determining step, the Court construes "generating from the client computer a Domain Name Service (DNS) request" as "generating and transmitting from the client computer a DNS request."

secure web computer

Asserted claims of the '135 Patent contain the term "secure web computer." VirnetX proposes "the target computer that hosts the secure web site." Microsoft proposes "the target computer, which requires authorization for access, and hosts the secure web site." The Court previously construed this term in *Cisco*.[7]

VirnetX argues that the Court should adopt its construction from *Cisco*. Docket No. 95 at 11. VirnetX objects to Microsoft's construction because another claim term, "secure web site," already requires authorization for access. *Id.* To include two such requirements, VirnetX argues, would be redundant or a mischaracterization of the invention. *Id.* at 11–12. In response,

[7] In *Cisco*, the Court construed "secure web computer" as "the target computer that hosts the secure web site." *Cisco*, Docket No. 266 at 23.

Microsoft argues that the requirement of authorization for access follows what VirnetX argued to the Court in *Cisco*. Docket No. 101 at 18–19. Microsoft also contends that an authorization requirement for a secure web site does not preclude a separate authorization requirement for a secure web computer. *Id.* at 20.

Microsoft is correct. The Court's previous construction of "secure web computer" focused on the meaning of "web computer" rather than on the meaning of "secure." Here, the parties specifically dispute the "secure" aspect and whether in this context it means "access authorization." The fact that a web site is "secure" does not mean that a web computer is also "secure." In the context of the intrinsic evidence, the term "secure" connotes access authorization. As VirnetX argued in *Cisco* and as Microsoft argues now, the term imposes a requirement for access authorization. Accordingly, the Court construes "secure web computer" as "the target computer, which requires authorization for access, and hosts the secure web site."

secure target computer

Asserted claims of the '135 Patent contain the term "secure target computer." VirnetX argues that no construction is necessary. Microsoft proposes "the target computer, which requires authorization for access, and hosts the secure web site."

The issue and arguments regarding this term are identical to those raised for the previous term ("secure web computer"). The Court explained in *Cisco* that the '135 Patent uses the terms "secure web computer" and "secure target computer" interchangeably. *Cisco*, Docket No. 266 at 23. Therefore, for the same reasons set forth above, the Court construes "secure target computer" as "the target computer, which requires authorization for access, and hosts the secure web site."

an indication that the domain name service system supports establishing a secure communication link[8]

Asserted claims of the '504 Patent contain the term "an indication that the domain name service system supports establishing a secure communication link." VirnetX argues that no construction is necessary, but alternatively proposes "an indication that the domain name service system has authorized and supports establishing a secure communication link." Microsoft proposes "an affirmative signal, beyond the signals required to establish a secure communication link, that the domain name service supports establishing a secure communication link." The Court previously construed this term in *Cisco*, *Mitel*, and *Apple*.[9]

Here, the parties dispute the meaning of "an indication." Microsoft argues that VirnetX made a disclaimer involving the term during reexamination. Docket No. 101 at 21–23. According to Microsoft, VirnetX unequivocally stated that any signal required to support establishing the secure communication cannot also serve as the claimed indication. *Id.* Therefore, Microsoft argues, the construction should reflect VirnetX's representation that the "indication" and "establishing" elements are separate and distinct. *Id.* VirnetX argues that there was no disclaimer during reexamination. Docket No. 95 at 12.

In *Apple*, the Court found that VirnetX's reexamination response constitutes an unequivocal disclaimer of DNS servers that only return requested DNS records, such as an IP address or key certificate. *Apple*, Docket No. 180 at 10. However, Microsoft's proposed construction does not correspond to the scope of the disclaimer. Additionally, Microsoft's

[8] This term is representative of several "indication" terms that only differ grammatically from one another. *See* Docket No. 83-2, Ex. B at 3. The Court resolves the parties' disputes and expects that the parties will apply this construction to the variants of this term.

[9] In *Cisco* and *Mitel*, the Court held that this term does not require construction. *Mitel*, Docket No. 347 at 10–11; *Cisco*, Docket No. 266 at 27–28. More recently, in *Apple*, the Court construed this term as "an indication other than merely returning of requested DNS records, such as an IP address or key certificate, that the domain name service system supports establishing a secure communication link." *Apple*, Docket No. 180 at 10.

proposal of an "affirmative signal" does not improve on the more precise construction given in the *Apple* case.[10]

The Court construes "an indication that the domain name service system supports establishing a secure communication link" as "an indication other than merely returning of requested DNS records, such as an IP address or key certificate, that the domain name service system supports establishing a secure communication link."

indicate in response to the query whether the domain name service system supports establishing a secure communication link[11]

An asserted claim of the '211 Patent contains the term "indicate in response to the query whether the domain name service system supports establishing a secure communications link." VirnetX argues that no construction is necessary, but alternatively proposes "indicate in response to the query whether the domain name service system has authorized and supports establishing a secure communication link." Microsoft proposes "sending an affirmative signal beyond the signals required to establish a secure communication link, that the domain name service supports establishing a secure communication link."

The issue and arguments regarding this term are identical to those raised for the previous term ("an indication that the domain name service system supports establishing a secure communication link"). Namely, VirnetX's response to a rejection during reexamination of the '211 Patent, which contains this term, is identical in relevant respects to the response to a rejection of the '504 Patent claims described above. *See Apple*, Docket No. 150-15, Ex. 14 at 5–6. Therefore, for the same reasons set forth above, the Court construes "indicate in response to

[10] At the hearing, Microsoft acknowledged that the Court's construction in *Apple* is a "very good step," but continued to argue that its proposal was simpler. Tr. Sep. 4, 2014, Docket No. 124 at 26:10–16.

[11] As in note 8, *supra*, this term is representative of several "indicate" terms that only differ grammatically from one another. *See* Docket No. 83-2, Ex. B at 4. The Court expects that the parties will apply this construction to the variants of this term.

the query whether the domain name service system supports establishing a secure communication link" as "indicate in response to the query, other than the mere returning of requested DNS records, such as an IP address or key certificate, that the domain name service system supports establishing a secure communication link."

intercept / intercepting

Asserted claims of the '151 Patent contain the term "intercept" or "intercepting." VirnetX argues that no construction is necessary. Microsoft proposes "access/accessing a communication addressed to another." At the hearing, the parties agreed that this term does not require construction, with the understanding that "intercepting" means more than simply "receiving." Tr. Sep. 4, 2014, Docket No. 124 at 36:9–37:3. The Court adopts the parties' agreement and clarifies that "intercepting" means more than "receiving." Given that clarification, the Court finds that "intercept" and "intercepting" do not require construction.

nonsecure computer

Asserted claims of the '151 Patent contain the term "nonsecure computer." VirnetX argues that no construction is necessary. Microsoft proposes "a computer that does not require authorization for access."

VirnetX argues that the parties' agreed construction of "secure server"[12] negates the need for a construction of "nonsecure computer." Docket No. 95 at 15. According to VirnetX, while "secure" means requiring authorization for access, it does not follow that the absence of authorization for access is a defining feature of a "nonsecure computer." *Id.* at 15–16. Microsoft argues that "nonsecure computer" is the opposite of "secure web/target computer."

[12] VirnetX and Microsoft agree that "secure server" should be construed as "a server that requires authorization for access and that can communicate in an encrypted channel." Docket No. 83-1, Ex. A.

Docket No. 101 at 28–29. Thus, it concludes, a "nonsecure computer" is a computer that does not require authorization for access. *Id.*

In the context of the intrinsic record and based on the Court's prior constructions, "secure" and "nonsecure" define whether or not authorization is required for access. Accordingly, the Court construes "nonsecure computer" as "a computer that does not require authorization for access."

DISPUTED TERMS FOR WHICH PARTIES REST ON PRIOR BRIEFING

For the remainder of the disputed terms, VirnetX and Microsoft rest on the claim construction briefing from the *Microsoft I, Cisco, Mitel*, and *Apple* cases. Docket No. 83 at 2; Docket No. 83-2, Ex. B. They raise no new arguments. Because the parties provide no reason to modify the Court's prior constructions and for the reasons stated in the *Microsoft I, Cisco, Mitel*, and *Apple* cases, the Court construes the remainder of the disputed terms as follows:

Claim Term	Court's Construction
domain name	a name corresponding to an IP address
between [A] the client and [B] the secure server between [A] the client computer and [B] the target computer between [A] a/the first computer and [B] a/the second computer	extending from [A] to [B]
secure communication link[13]	a direct communication link that provides data security and anonymity
web site	one or more related web pages at a location on the World Wide Web
secure web site	a web site that requires authorization for access and that can communicate in a VPN
virtual private link	a virtual private network as previously defined

[13] The Federal Circuit construed this term in *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1316 (Fed. Cir. 2014). The Court adopts the Federal Circuit's construction.

Microsoft I, Docket No. 246; *Cisco*, Docket No. 266; *Mitel*, Docket No. 307; *Apple*, Docket No. 180.

CONCLUSION

For the foregoing reasons, the Court interprets the claim language in this case in the manner set forth above. For ease of reference, the Court's claim interpretations are set forth in a table in Appendix A and the parties' agreed constructions are set forth in a table in Appendix B.

So ORDERED and SIGNED this 17th day of December, 2014.

LEONARD DAVIS
UNITED STATES DISTRICT JUDGE

APPENDIX A

Claim Term	Court's Construction
virtual private network (VPN)	a network of computers which privately and directly communicate with each other by encrypting traffic on insecure paths between computers where the communication is both secure and anonymous
domain name service (DNS)	a lookup service that returns an IP address for a requested domain name to the requester
secure domain name	a non-standard domain name that corresponds to a secure computer network address
secure domain name service	a non-standard lookup service that recognizes that a query message is requesting a secure computer address, and returns a secure computer network address for a requested secure domain name
DNS proxy server	a computer or program, separate from the client application, that responds to a domain name inquiry in place of a DNS
domain name server (DNS) proxy module	a computer module or program module, separate from the client application, that responds to a domain name inquiry in place of a DNS
generating from the client computer a Domain Name Service (DNS) request	generating and transmitting from the client computer a DNS request
secure web computer	the target computer, which requires authorization for access, and hosts the secure web site
secure target computer	the target computer, which requires authorization for access, and hosts the secure web site
an indication that the domain name service system supports establishing a secure communication link	an indication other than merely returning of requested DNS records, such as an IP address or key certificate, that the domain name service system supports establishing a secure communication link
indicate in response to the query whether the domain name service system supports establishing a secure communication link	indicate in response to the query, other than the mere returning of requested DNS records, such as an IP address or key certificate, that the domain name service system supports establishing a secure communication link
intercept / intercepting	No construction necessary. The Court clarifies that "intercepting" means more than simply "receiving."

Claim Term	Court's Construction
nonsecure computer	a computer that does not require authorization for access
domain name	a name corresponding to an IP address
between [A] the client and [B] the secure server between [A] the client computer and [B] the target computer between [A] a/the first computer and [B] a/the second computer	extending from [A] to [B]
secure communication link	a direct communication link that provides data security and anonymity
web site	one or more related web pages at a location on the World Wide Web
secure web site	a web site that requires authorization for access and that can communicate in a VPN
virtual private link	a virtual private network as previously defined

APPENDIX B

Claim Term	Agreed Construction
secure target web site	a secure web site on the target computer
automatically initiating the VPN	initiating the VPN without involvement of a user
secure computer network address	a network address that requires authorization for access and is associated with a computer capable of virtual private network communications
automatically initiating an encrypted channel / automatically creating an encrypted channel / automatically creating a secure channel	[initiating/creating] the [encrypted channel/secure channel] without involvement of a user
secure server	a server that requires authorization for access and that can communicate in an encrypted channel
enable establishment of a secure communication link . . . transparently to a user at the first location	the user at the first location need not be involved in enabling establishment of the secure communication link
secure network address	a network address that requires authorization for access and is associated with a computer capable of virtual private network communications